DEFECT REPORT FORM

1. Defect Report Number: 9594/176

   Title: **Access controls on aliases**

2. Source: ITU Rapporteur for Q15/7 Source No. ITU-12

3. Addressed to: ISO/IEC JTC1/SC21/WG8 and ITU-T Study Group 7
   Editor Group on the Directory

4. (a) WG Secretariat: ANSI
   (b) ITU-T WP: SG 7/WP 4

5. Date Circulated by WG Secretariat:

6. Deadline for Response from Editor:

7. Defect Report Concerning:

   X.511 (1993) & IS 9594-3 (1995) The Directory - Abstract Service

8. Qualifier: Ambiguity

9. References in Document:

   Clause 7.11.1

10. Nature of Defect:

    Inconsistent results may be obtained when one DSA holds an alias to an entry in another DSA and access controls are set up in a particular way. Assume DSA1 holds an alias to an entry in DSA2, and that the access permissions on the **aliasedEntryName** attribute are such as to *deny* read access, but the permissions on the entry itself are to *grant* access.

    Then a read operation on the alias name (with alias dereferencing) will return the entry in DSA2 if DSA2 is up (Case A), but will return a **nameError** (no such entry) if DSA2 is down (Case B).

    It would be more consistent to either return a **nameError** whenever the entry is accessed through its alias and the alias denies read access (Case A), or to consistently ignore alias permissions and return a **referral** if DSA2 is down (Case B).

    Although the situation of having an alias deny read access but having the entry grant it is unusual, it is undesirable to have such an inconsistency in the Directory’s behaviour.

11. Solution Proposed by the Source:

    Change 7.11.1 to mandate the read entry and read aliasedEntryName attribute access control requirements in all cases, not only if a referral is to be returned.

12. Editor's Response: